

Remarks

This Amendment is submitted in connection with a Request for Continued Examination ("RCE"), filed July 11, 2005. The RCE continues examination following a final Office action, mailed April 11, 2005. In that action, claims 2-4, 6-14 stand rejected.

With this Amendment, claims 2-4, 7 and 10-14 have been amended to further explicate the subject matter. In addition, new claims 15-28 have been added. These amendments introduce no new matter. Applicant respectfully requests, in light of the claim amendments above and the remarks that follow, that this application be reconsidered, that the rejections be withdrawn and that this case be advanced to issue.

Applicant notes that, in devices performing cryptographic algorithm, important information (e.g., cryptographic keys) may be revealed to an attacker by application of statistical analysis to the device's operation, including its inputs, outputs and consumption characteristics (e.g., power, current, other indirect radiations). Among other things, Applicant addresses vulnerability of the device to such attacks by impeding analysis of the current consumption characteristics associated with the operations and/or sub-operations of the cryptographic algorithm. That is, Applicant provides for execution of a cryptographic operation (or sub-operation) simultaneously with a second operation, so that the consumption characteristics of the data-processing device is a superimposition of consumption characteristics associated with performing the cryptographic operation and consumption characteristics associated with performing the second operation. Applicant also contemplates provision of a second operation having associated consumption characteristics that are complementary with consumption characteristics associated with performing the cryptographic operation.

The action rejects claims 2, 4, 7, 9 and 10-13 under 35 USC 103(a) as unpatentable over Patarin in view of Jahnich. The action further rejects claims 3, 6, 8 and 14 under 35 USC 103(a) as unpatentable over Patarin in view of Jahnich and further in view of Tan. The action

cites Patarin to establish (a) execution of operations simultaneous and in parallel (see the action's reference to Patarin's Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40) and (b) combination of sub-results to an overall result of the overall cryptographic operation (see the action's references to Patarin's Fig. 2, step B; col. 12, lines 6-12 and 31-40).

However, the Office action fails to establish a prima facie case of obviousness. To properly establish a prima facie case of obviousness, the Office action must establish three basic criteria. First, the Office action must identify suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, which supports modifying the references or combining the references' teachings. Second, in so modifying/combining, a reasonable expectation of success must exist. Third, the prior art reference (or references when combined) must teach or suggest all the claim limitations. Even with these criteria met, the Office action establishes a prima facie case of obviousness only if the teaching or suggestion to make the combination/modification and the reasonable expectation of success are both found in the prior art, rather than being based on applicant's disclosure. In re Vaack, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Here, the Office action does not meet the three criteria, and the combinations/modifications appear to be based on applicant's disclosure.

To illustrate, the Office action omits to identify where Patarin discloses, or even contemplates, impeding, through superimposition or otherwise, reconstruction of the consumption characteristics associated with performing the cryptographic operation, as claimed in Applicant's application.

Indeed, in addressing protection, Patarin appears to take a completely different approach than does Applicant. While it implements a standard cryptographic algorithm, Patarin proposes a process that protects the system by significantly modifying the algorithm (see, e.g., Fig. 3A, 3C and related text). Patarin separates that standard algorithm into several new

calculation parts, so as to produce partial intermediate results distinct from the intermediate results of the standard algorithm. Patarin proposes that the computer system is protected because typical attacks generally rely on exploiting the existence of established intermediate results (i.e., because the algorithm's are standard). With the Patarin's modifications to the algorithms, the attacks fail because the intermediate results no longer exist, being replaced with the distinct partial intermediate results. Patarin's approach is mathematically intense and relatively complex (e.g., separating each known intermediate variable into two new variables, applying permutations on these new variables, etc.).

By comparison to Patarin, Applicant implements the standard algorithm without adding new calculation parts or other modification. Indeed, Applicant implements the standard algorithm so as to include the known intermediate results. Instead of modifying the algorithm (and increasing the complexity associated therewith), Applicant protects against attacks by, as previously described, impeding reconstruction of consumption characteristics associated with performing the algorithm's standard cryptographic operations (or known sub-operations). Moreover, even where Applicant discloses splitting cryptographic operations, those splits are based on the algorithms known sub-operations, such that the sub-operations are executed without modification.

The Office action cites Jahnich to fill a cited gap Patarin. That is, the Office action states that Patarin does not teach use of dummy operations in cryptographic operations. The Office action states that Jahnich discloses using dummy programs whose execution does not influence an encryption result.

Jahnich appears to propose to secure portable data carriers (e.g., smart cards) simply by permuting the serial order of execution of at least certain subprograms within a standard encryption program. Jahnich further proposes to supplement the encryption program with at least one dummy program, the dummy program being permuted into the serial order.

While Jahnich provides the Office action with a patent from which the "dummy program" element can be combined to fill Patarin's cited gap, the Office action recites insufficient basis to do so. That is, nowhere does the Office action set forth any sufficient suggestion or teaching in Jahnich or Patarin to support the action's conclusion that it would be obvious to modify Patarin's complex process to use the dummy programs of Jahnich. Indeed, the action appears to combine so as to merely assemble the elements of Applicant's claims.

Moreover, nowhere does the Office action describe how Patarin's process would be modified to include such dummy programs. Indeed, notwithstanding the mathematical complexity of the Patarin process, the Office action omits both any basis to support that Patarin can actually be modified as the action suggests and, assuming that modification might be possible, any statement on how to do so while still effecting (and successfully) Patarin's proposals.

In addition, nowhere does the Office action recite any suggestion, teaching or description beyond a mere use of "dummy programs". That is, the Office action omits any recitation directed to Applicant's claimed use of dummy operations, e.g., as part of a superimposition of consumption characteristics so that reconstruction of the consumption characteristics associated with performing the cryptographic operation is impeded.

The Office action cites Tan to fill another cited gap, here left by both Patarin and Jahnich. That is, the Office action states that Patarin and Jahnich do not teach either that (a) selection of a processor to perform certain cryptographic operations is randomly controlled (i.e., the action refers to Tan at col. 3, lines 60-64 and col. 6, lines 6-12) or (b) split up of the cryptographic operation is randomly controlled (i.e., the action refers to Tan at col. 3, lines 8-42).

While Tan provides the Office action with a patent from which the "random control" element can be combined to fill the cited gap, the action recites insufficient basis to do so. That is, nowhere does the Office action set forth any sufficient suggestion or teaching in Tan, Jahnich

or Patarin to support the action's conclusion that it would be obvious to modify Patarin's complex process so as to use the "random control" of Tan. Indeed, the action appears to combine so as to merely assemble the elements of Applicant's claims.

Moreover, while the words alone are similar, the "random control" of Tan is not the element of Applicant's claims. The Office action's first cited references to Tan appear to propose only a method for constructing an encryption algorithm from a group of suitable algorithms. Therein, the random generator is used to select one algorithm from among such suitable algorithms or, equivalently, to select one from among plural processors, each of which processor has an associated such suitable algorithm. Accordingly, here, the Office action omits any recitation in Tan directed to Applicant's claimed use of random controlling selection of processor to perform cryptographic and/or second operations (e.g., the same or different cryptographic operation, or some dummy operation), which selection is toward impeding reconstruction of consumption characteristics associated with performing cryptographic operations.

In turn, the Office action's second cited references to Tan appear to be directed to selecting among sub-keys for encrypting different data blocks (see Tan, col. 3, lines 61-62). Again, as above, the Office action omits any recitation directed to Applicant's claimed use of random control to split known operations into sub-operations, which selection is toward impeding reconstruction of consumption characteristics associated with performing cryptographic operations.


Applicant herewith re-iterates the remarks set forth in its previous response. Applicant respectfully requests reconsideration of those previous remarks, particularly in light of the remarks and claim amendments of this document. Applicant draws specific attention to the previous remarks, at page 10, first paragraph.

Applicant also re-iterates that nothing herein is to be deemed either acquiescence in any rejection in any Office action, or a waiver or arguments not set forth herein. Applicant further re-iterates its reservation of the right and intent to prosecute any and all subject matter embodied in the originally filed claims, including via subsequent continuing application(s).

CONCLUSION

Applicant submits that in view of the foregoing remarks and/or amendments, the application is in condition for allowance, and favorable action is respectfully requested. As to this Amendment, the Commissioner is hereby authorized to charge any fees, including extension fees, which may be required, or credit any overpayments, to Deposit Account No. 50-1001.

Respectfully submitted,



Michael E. Schmitt
Registration No. 36,921
P. O. Box 2200
Hillsboro, OR 97123
Telephone: (503) 844-9009
Facsimile: (503) 296-2172
email: mail@ganzlaw.com

Date: July 14, 2005

Correspondence to:

Philips Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131 USA
Telephone: (408) 474-9073
Facsimile: (408) 474-9082
USPTO Customer Number: 24738